УДК 004.056.5

О ВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ОСОБЕННЫХ ТОЧЕК В ИЗОБРАЖЕНИИ ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ

Мухамедьянов И.Р.,
научный руководитель канд. физ.-мат. наук Дмитриев В.Л.
Стерлитамакский филиал Башкирского государственного университета

В настоящее время, наряду с широким использованием цифровых форматов мультимедиа и существующими проблемами управления цифровыми ресурсами, становятся все более актуальными исследования в области стеганографии. На сегодняшний день существует довольно много программных продуктов, применяемых для целей стеганографии и реализующих методы внедрения конфиденциальных данных в различные типы файлов.

Классическая задача стеганографии состоит в организации передачи секретного сообщения таким образом, чтобы как содержание сообщения, так и сам факт его передачи были скрыты ото всех, кроме заинтересованных лиц. Для решения такой задачи используется некоторое сообщение, называемое контейнером (стего-контейнером), в которое встраивается требуемое для передачи секретное сообщение. При этом разработчики стеганографических методов должны организовать прозрачность передаваемых конфиденциальных данных: изменение определенного числа информационных бит в контейнере не должно привести к особым потерям его качества (должны отсутствовать артефакты визуализации встраивания).

Хотя в компьютерной стеганографии в качестве контейнера может выступать практически любой файловый формат, однако наиболее распространенным типом носителя являются файлы изображения формата BMP. Это объясняется тем, что для целей стеганографии наиболее предпочтительны файлы форматов, в которых используются методы сжатия без потерь (такие виды сжатия типичны для изображений формата BMP, TIFF, PNG, TGA, и др.). Также положительной стороной в пользу выбора формата BMP выступает высокое качество изображения и простота формата.

Стоит отметить, что при работе с форматами файлов, использующих сжатие с потерями, таким как JPEG, обычно все равно выполняют преобразование потока данных JPEG в поток данных BMP. С позиции стеганографии файлы данного формата позволяют скрывать сравнительно большие объемы информации.

В данной работе в качестве контейнера рассматривается 24-битовое растровое изображение в системе цветности RGB. Каждая цветовая комбинация тона (пикселя) представляет собой комбинацию значений яркости трех составляющих цветов – красного (R), зеленого (G) и синего (B), которые занимают каждый по 1 байту (итого по 3 байта на точку). Таким образом, яркость каждой составляющей записывается 8-битным числом и может изменяться в диапазоне от 0 до 255 (комбинация (0, 0, 0) соответствует черному цвету, комбинация (255, 255, 255) – белому). Использование BMP-файлов в настоящей работе обусловлено только лишь простотой их программной обработки, – все полученные результаты с легкостью могут быть перенесены на случай изображений в файлах других форматов.

Самым распространенным на сегодня методом стеганографического скрытия является метод замены наименее значимых бит (LSB). Традиционно LSB-методы реализуются по следующей схеме: передаваемое сообщение шифруется с использованием секретного ключа, после чего биты зашифрованного сообщения записываются на место младших бит цветовых составляющих изображения. Визуально, в таком изображении не будет заметно никаких искажений, однако компьютерные методы стегоанализа смогут определить наличие встроенного сообщения (например, метод стегоанализа, пред-

ложенный М.Ю. Жилкиным и относящийся к классу универсальных методов). Поэтому в ряде работ предлагаются варианты LSB-методов, более устойчивых к стегоанализу. Таковым является, например, метод, учитывающий статистику младших бит изображения.

В данной работе предлагается метод, использующий распределение в изображении некоторых особенных точек (отсутствующих в исходном изображении оттенков).

На первом этапе необходимо подготовить контейнер к приему скрытого сообщения – в исходном файле изображения, составляющие (оттенки) трех цветов, имеющие значения 255, изменяются на 254. На этом же этапе скрываемое сообщение переводится в двоичную последовательность.

На втором этапе проводится анализ файла-контейнера на наличие точек, удовлетворяющих следующему условию: во всем изображении два оттенка цвета точек (например, синий (B) и зеленый (G)) совпадают, а третий оттенок (в данном случае красный (R) – обозначим его числовое значение через X) таков, что во всем изображении нет точек, для которых значение этого оттенка равно X+1, X-1, или X-2. Среди всех найденных таким образом точек выбирается последовательность точек, имеющая максимальную длину. Такая последовательность и используется для хранения скрытого сообщения: к значению X третьего оттенка прибавляется соответствующее значение из двоичного представления сообщения. Данный метод был назван нами методом отсутствующих бит. При этом первые три байта сообщения содержат информацию о длине сообщения. Первая точка из найденной последовательности должна быть оставлена без изменений.

Очевидно, что для каждого потенциального файла-контейнера распределение точек, удовлетворяющих отмеченному выше требованию по оттенкам, вполне случайно. В связи с этим данный метод не вносит существенных отклонений в статистику распределения младших бит изображения, и должен быть вполне устойчив к методам стегоанализа.

После добавления сообщения в файл-контейнер исходный пустой контейнер уже не требуется и может быть удален. Таким образом, данный метод позволяет использовать для передачи (и последующего восстановления) скрытого сообщения только один файл. Восстановление сообщения основывается на поиске во всем изображении точек, два оттенка цвета которых совпадают, а третий оттенок таков, что во всем изображении нет точек, для которых значение этого оттенка равно X-1 или X-2.

При таком способе сокрытия информации максимальный ее объем, который может быть размещен в файле-контейнере, целиком зависит от файла изображения: какое-то изображение позволит сохранить больше информации – какое-то меньше (или вообще не позволит). Кроме того, само расположение скрытого сообщения в файле-контейнере будет также зависеть от конкретного изображения.

Для увеличения емкости контейнера можно использовать не только последовательность точек максимальной длины, но и все другие последовательности точек, удовлетворяющие указанному выше условию. Наряду с использованием секретного ключа это позволит повысить стойкость алгоритма к стегоанализу.

В ходе программной реализации предложенного метода в среде визуального программирования Delphi для доступа к точкам изображения использовалось свойство битовой карты TBitMap – ScanLine. Это свойство представляет собой массив указателей на строки с данными битовой карты (строки точечного изображения). Само значение свойства ScanLine изменить нельзя (оно доступно только для чтения), но можно изменить данные, на которые оно указывает. Таким образом, мы будем получать цвет пикселя непосредственно из области памяти, в которую записано изображение, что существенно ускоряет процесс анализа потенциального файла-контейнера.